Q1 Team Name

0 Points

INSYNC

Q2 Commands

10 Points

List the commands used in the game to reach the ciphertext.

exit1
exit3
exit4
exit4
exit1
exit3
exit4
exit1
exit3
exit2
read

Q3 Analysis

60 Points

Give a detailed description of the cryptanalysis used to figure out the password. (Use Latex wherever required. If your solution is not readable, you will lose marks. If necessary the file upload option in this question must be used TO SHARE IMAGES ONLY.)

When we just entered in level-6 we got message like " You are in a small chamber. Unlike the previous hall, this chamber seems naturally formed.... Going closer to an open exit, you notice "Exit 2" written on the wall next to it. Curious, you go around and find that

the exits are numbered from 1 to 5 in this fashion. The closed exit is numbered 5 and the exit from which you came in is numbered 1." It gave us hint that we have to use $exit1$ command to further proceed in game.After entering this we got message on screen "You travel through a twisted, narrow, and rocky passage that sometimes goes up, sometimes down, sometimes left, and sometimes right." and hexadecimal block $59|6f|75|20|73|65|65$ we stored it and moved further in game.Further we used $exit3$ command and got hexadecimal block as $20|61|20|47|6f|6c|64$. Then we used $exit4$ command and got hexadecimal block as $2d|42|75|67|20|69|6e$. Further we used $exit4$ command and got hexadecimal block as $20|6f|6e|65|20|63|6f$. Then we used $exit1$ and got hexadecimal block as $72|6e|65|72|2e|20|49$. Further we used $exit3$ and got hexadecimal block as $74|20|69|73|20|74|68$. Then we used $exit4$ command and got $65|20|6b|65|79|20|74$ and Then we used $exit1$ command and got hexadecimal block as $6f|20|61|20|74|72|65$. Further we used $exit3$ and got hexadecimal block as $61|73|75|72|65|20|66$. Then we used $exit2$ and got hexadecimal block as $6f|75|6e|64|20|62|79$.

-> After which we used $read$ command which gave us message as follows: $n =$ 84364443735725034864402554533826279174703893439763

INSYNC: This door has RSA encryption with exponent 5

->All the collected hexadecimal blocks were converted to ASCII and we got the text as "You see a Gold-Bug in one corner. It is the key to a treasure found by"

->As we got a hint on the screen that "This door has RSA encryption with exponent 5 and the password is" which simply states that we have to deal with RSA encryption. RSA is a public-key algorithm, named after its inventors Rivest, Shamir, and Adelman (RSA).

->Encryption $\longrightarrow c = m^e \ mod \ n$

->Decryption $\longrightarrow m = c^d \ mod \ n$

->Decryption Process of RSA Algorithm steps are as follows:
1) Obtain factors of n.
2) Find d, This requires euler's totient $\Phi(n) = (p-1) * (q-1)$
Now (1) is not possible due to the prime factorization problem. (2) is also not possible as we cannot find the factors.
Then, as the exponent is 5, we proceed as follows:
->Checking for "Copper-Smith's Attack : Low exponent attack", we first checked whether there is any padding added to the text or not. We computed the value of $c^{\frac{1}{e}}$ which turned out to be non-integer hence we concluded that padding has been added to the text.if we assume padding added to be x then our new encryption equation will look like this:
-> Encryption $\longrightarrow c = (x+m)^e \ mod \ n$
-> Known values in equation mentioned above as c, e, n, As e is very small we used Copper-Smith's algorithm to explore x. The Algorithm says that $n^{e^{-1}}$ is a very small root and can be obtained very easily.
->Copper-Smith's Attack : Let n be an integer and f be a polynomial of degree δ. Given n and f one can recover in polynomial time all x_0 satisfying $f(x_0)$ = (0 mod n). and $x_0 < n^{\frac{1}{\delta}}$, Therefore the final problem boils down to $f(m) = (x + m)^e \ mod \ n$.

->We have used SageMath inorder to use "fplll" library. Initially we require a major part of the message x and we need to find $m < n^{e^{-1}}$ which is going to be our password. We had collected two strings while struggling through various commands in game which are as follows
a. "You see a Gold-Bug in one corner. It is the key to a treasure found by"
b. "INSYNC: This door has RSA encryption with exponent 5 and the password is "

->x_{bin} is binary version of padding x.
->We assumed that the length of password m is less than $n^{\frac{1}{e}} \approx 4*10^{61}$ thus, we concluded that m can't be longer than $\lceil 4*10^{61} \rceil$ which is 205 bits. So, we get our polynomial as, $f(m) = ((x_{bin} < length(m)) + m)^e - c$. Root of the above polynomial is the required password which is calculated using Coppersmith's Algorithm and LLL (Lattice reduction).

->We tried both the strings mentioned in earlier steps but the 2nd string gave us a meaning root.
INSYNC: This door has RSA encryption with exp
. We got the root to be
0100001100111000010110010101000000110111011011110

Finally we took 8 bit blocks at a time & decoded them via ASCII value and got final password as "$C8YP7oLo6Y$"
We took the idea from the following references and codes for writing insync.sage.
References :
[1] https://doc.sagemath.org/html/en/tutorial/
[2]http://defeo.lu/sage-lattices-EJCIM/
[3] https://github.com/mimoo/RSA-and-LLL-attacks/blob/master/coppersmith.sage
[4] https://link.springer.com/content/pdf/10.1007/BFb0024458.pdf

No files uploaded

Q4 Password
10 Points

What was the final command used to clear this level?

C8YP7oLo6Y

Q5 Codes
0 Points

It is MANDATORY that you upload the codes used in the cryptanalysis. If you fail to do so, you will be given 0 for the entire assignment.

INSYNC.zip Download

```
1  Binary file hidden. You can download it using the button above.
```

Assignment 6

GRADED

GROUP

Aman Mittal
Piyush Gangle
Punit Chaudhari

View or edit group

TOTAL POINTS

80 / 80 pts

QUESTION 1

Team Name — **0** / 0 pts

QUESTION 2

Commands — **10** / 10 pts

QUESTION 3

Analysis — **60** / 60 pts

QUESTION 4

Password — **10** / 10 pts

QUESTION 5

Codes — **0** / 0 pts